(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 August 2005 (18.08.2005)

PCT

(10) International Publication Number
WO 2005/076522 A1

(51) International Patent Classification[7]: H04L 9/32

(21) International Application Number:
PCT/DK2005/000090

(22) International Filing Date: 10 February 2005 (10.02.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

PA 2004 00201	10 February 2004 (10.02.2004)	DK
60/542,861	10 February 2004 (10.02.2004)	US
PA 2004 00975	22 June 2004 (22.06.2004)	DK
60/581,354	22 June 2004 (22.06.2004)	US

(71) Applicant *(for all designated States except US)*: **CRYPTICO A/S** [DK/DK]; Frubjergvej 3, DK-2100 Copenhagen Ø (DK).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **SØRENSEN, Hans Martin Boesgaard** [DK/DK]; Ulrikkenborg Plads 10A, 1.tv., DK-2800 Lyngby (DK).

(74) Agent: **INSPICOS A/S**; Bøge Allé 5, P.O. Box 45, DK-2970 Hørsholm (DK).

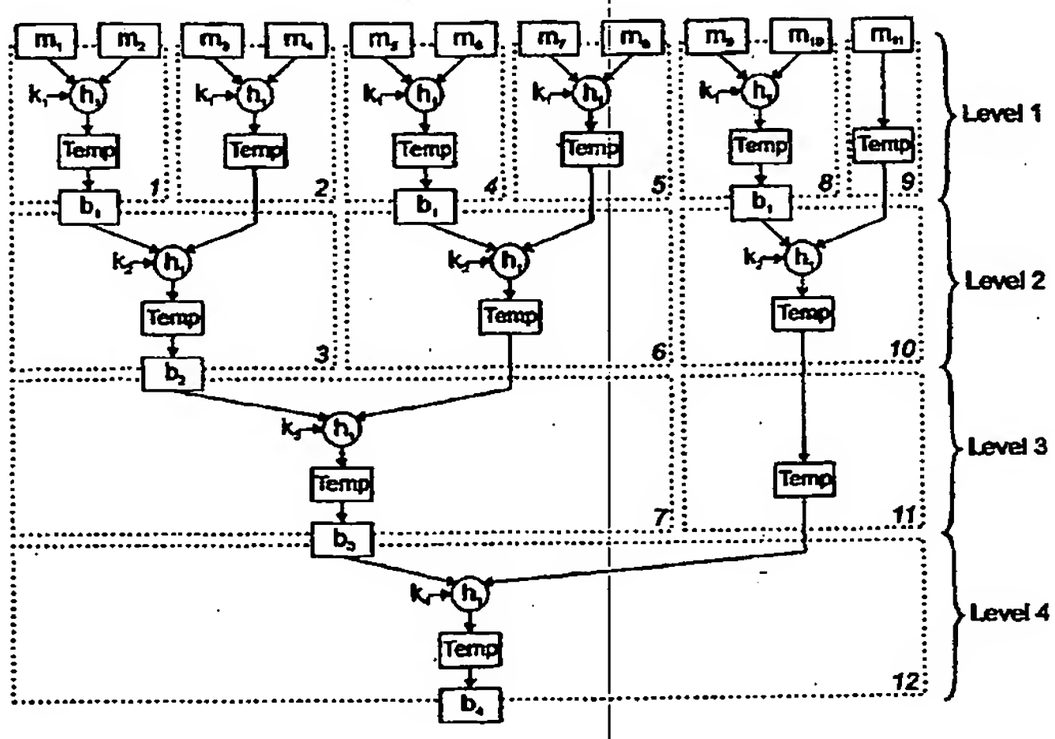
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) **Title:** METHODS FOR GENERATING IDENTIFICATION VALUES FOR IDENTIFYING ELECTRONIC MESSAGES



(57) **Abstract:** In a method for generating an identification value for identifying an electronic message by application of a first hash function with fixed compression that compresses n blocks of data into a number of blocks, which is smaller than n, the hash function is repetitively applied in a tree-structure compression of the message. The message is compressed in a plurality of tree structure levels, each level receiving m_i input blocks for compression. One or more residual data blocks are treated by an auxiliary hash function or passed without compression from the current level to another subsequent level, in case n does not divide the number of input blocks at a particular level. A further method is provided, in which a number representation of a block of data is added to a number resulting from a hash operation. The methods of the invention may define MAC (Message Authentication Code) functions.

WO 2005/076522 A1